UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/701,157	11/03/2003	Robert N. Nazzal	12221-026001	5548

26161 7590 02/08/2008
FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
GEE, JASON KAI YIN	
ART UNIT	**PAPER NUMBER**
2134	

MAIL DATE	DELIVERY MODE
02/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/701,157	NAZZAL, ROBERT N.	
	Examiner	Art Unit	
	Jason K. Gee	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 December 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/05/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is response to communication: filed on 12/05/2007 with acknowledgement of benefit date of 11/04/2002.

2. Claims 1-25 are currently pending in this application. Claims 1, 10, and 22 are independent claims.

3. The IDS received 12/05/2007 has been accepted.

Response to Arguments

4. Applicant's arguments filed 12/05/2007 have been fully considered but they are not persuasive.

As per claim 1, the applicants have amended the preamble to recite that the GUI is rendered on a display associated with an IDS. Amending the preamble does not add to the claim limitations. However, even if these limitations were to be considered, the prior art teaches this, as a GUI is inherently rendered on display. As seen in the figures of the references, the figures represent what is being rendered on a display (if not, nothing can be seen). The applicants also argue that the references teach a virus protection program and not an intrusion detection system. However, again, the intrusion detection system is not claimed, as it is merely in the preamble. Further, as most broadly interpreted, a virus is an intruder into a system. Even more, paragraph 37 teaches that it spots intruder access, and it operates based on network changes. The applicant also argues that the combination does not teach a snooze function. However, Symantec teaches this by showing the 'remember' function, which allows an action to

continue for a certain period of time. These may be later edited in time, if the user actually deems them suspicious or malicious, as taught by Symantec on 5-7, and thus, would be useful with the Cooper combination. Therefore, the combination teaches all the claimed limitations. This woudl be useful, as stated earlier, as not all suspicious activity alerts necessarily mean there is malicious activity; therefore, it would be advantageous to snooze these alerts to deal with later in case they really are issues.

As per claim 2, the applicants argue that Cooper does not teach alerts based on grouping or roles of hosts. However, as cited in the previous office action, security policies based on roles of hosts are taught in Cooper in paragraph 100 and 158. Paragraph 100 teaches wherein policy may be based on communites of hosts, servers, subnets and firewalls, as well as service level. Also, as seen in table A in paragraph 86, communites of hosts are grouped together when they have similar functions/roles.

As per clam 4, Cooper does indeed teach that GUIs are used to depict anomalies that were used to classify the event, in Figure 12. The disposition, such as an invalid url, probable scan, are anomalies.

As per claim 10 as amended, the applicants argue that Billhartz does not teach event severity having a percentage relationship to an estalished threshold. However, this is taught in col. 8 lines 40 to col. 9 line 10, as stated in the previous Office Action. The event severity may be an intruder, and this is based on the threshold or percentage of collisions in a given amount of time.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-9 and 22-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper US Patent Application Publication 2002/0069200 (hereinafter Cooper), and in view of Symantec's *Symantec Antivirus for Macintosh SAM*, 1994, (hereinafter Symantec).

As per claim 1, Cooper teaches a graphical user interface rendered on a display associated with an intrusion detection system, the graphical user interface comprising: a field that depicts a summary of anomalies identified as part of a event that is detected in a network (throughout the reference, such as Figure 26, paragraph 514, abstract, paragraph 42), the summary indicating event severity details of the event (Figure 26). However, at the time of the invention, Cooper does not explicitly teach an alert action region including a control to permit a user to snooze future alerts related to the event in the summary for a period of time. A snooze for future alerts is taught Symantec though, such as in pages 4-9 and 5-6, wherein an event may be allowed to continue, and an alert may be prevented from appearing in the future.

At the time of the invention, it would have been obvious to combine the teachings of Cooper with Symantec. One of ordinary skill in the art would have been motivated to perform such an addition, as some anomalies are not necessarily a sign of malicious

activity. If this is the case, it would be beneficial to snooze these alerts, as they are not malicious, and it would be more convenient to the user. Symantec teaches in 5-6 that not all suspicious activity alerts necessarily means there is malicious activity.

As per claim 2, Symantec teaches wherein the snooze control feature can be selected based on event types (4-9 and 5-6, such as when events occur when copying programs). Cooper then teaches the preventing of unnecessary alerts due to roles of hosts, such as in paragraphs 100 and 158.

As per claim 3, Symantec teaches clearing alerts if the alerts appear on the overview page (pages 5-6 and 4-9). Also, this is taught by Cooper in Figure 28, wherealerts may be cleared on an overview page with an aggregated view of the network status.

As per claim 4, Cooper teaches wherein an event details region of the graphical user interface depicts anomalies that were used to classify the event (Figure 22).

As per claim 5, Cooper teaches wherein details of events include values of source (Figure 23), destination (Figure 23), and protocol that caused an event to be raised (Figure 24).

As per claim 6, Cooper teaches wherein event severity is coded by an indicia (Figures 22, 25, 26, paragraph 520).

As per claim 7, Symantec teaches a control to clear a selected alert (4-9 and 5-6). This is also taught in Cooper, such as in paragraph 594

As per claim 8, Cooper teaches wherein the interface includes a details control that allows a user to observe details about a selected anomaly (Figures 26 and 27, wherein a view button is available to view details).

As per claim 9, Cooper teaches wherein the details control presents a list of IP addresses to which the host attempted to connect (Figures 27, 29, 30 and throughout the reference).

Independent claim 22 is rejected using the same basis of arguments used to reject claim 1 above.

Claim 23 is rejected using the same basis of arguments used to reject claim 2 above.

Claim 24 is rejected using the same basis of arguments used to reject claim 7 above.

Claim 25 is rejected using the same basis of arguments used to reject claim 8 above.

7. Claims 10-14 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper and Symantec as applied above, and further in view of Billhartz US Patent No. 6,986,161 (hereinafter Billhartz).

Independent claim 10 is rejected using the same basis of arguments used to reject claim 1 above. However, Cooper and Symantec do not explicitly teach an event severity having a percentage relationship to an established threshold for issuing an

event notification. This is taught throughout Billhartz though, such as in col. 8 line 41 to col. 9 line 10.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include basing event notifications on percent relationships. One of ordinary skill in the art would have been motivated to perform such an addition to provide greater certainty when issuing alerts, thereby reducing false positives. As indicated in col. 2 liens 15-23 of Billhartz, the previous intrusion detections systems do not reliably indicate whether some nodes are rouge or legitimate nodes.

As per claim 11, Symantec teaches an event to be snoozed for a fixed period of time (pages 4-9, 5-6, and 5-7).

Claim 12 is rejected using the same basis of arguments used to reject claim 2 above.

Claim 13 is rejected using the same basis of arguments used to reject claim 7 above.

Claim 14 is rejected using the same basis of arguments used to reject claim 8 above.

As per claim 18, as best understood by the Examiner, details of source and destination populated with IP addresses is taught throughout Cooper, as can be seen in Figures 23. Cooper then teaches the preventing of unnecessary alerts due to roles of hosts, such as in paragraphs 100 and 158.

8. Claims 15-17 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper, Symantec, and Billhartz, as applied above, and further in view of Porras US Patent No. 6,321,338 (hereinafter Porras).

As per claim 15, the Billhartz combination teaches all of the previous limitations, and the GUI interface for detecting intruders. However, it does not teach indicating normal operating conditions of a host and current operating conditions of a host. Comparing these two are taught throughout Porras, such as in col. 2 lines 25-35; col. 6 lines 39-60; and col. 8 line 65 to col. 9 line 7.

At the time of the invention, it would have been obvious to combine the teachings of Porras with the Billhartz combination. Porras teaches creating long term statistical profiles ('normal' operating conditions), and comparing them with short term statistical profiles ('current' operating conditions). By doing so, network intrusion can be detected with greater accuracy and would provide greater security to networks (col. 2 lines 40-68).

As per claim 16, Porras teaches a comparison between normal and current connection rates of the host (col. 6 lines 1-20). The displaying of such features is taught by the Billhartz combination, as indicated earlier.

As per claim 17, Porras teaches throughout the reference events such as historical anomaly, as it compares previous long term statistical profiles. Porras also teaches event types like worm propagation, such as in col. 4 lines 25-48. Further, Porras teaches event types such as denials of service (col. 1 lines 55-65, col. 13 line

60-col. 14 line 7). Cooper teaches unauthorized access throughout the reference, and for example, can be seen in Figure 22.

As per claim 21, as best understood by the examiner, Porras teaches wherein a statistical measure is a number of bytes per second and packets per second of each type of protocol observed in the system (col. 5 lines 30-37).

9. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper, Symantec, and Billhartz, as applied above, and further in view of Central Point's *Central Point Anti-Virus – Virus detection, Removal and Prevention*, 1991 (hereinafter Central Point).

As per claim 19, the Billhartz combination does not explicitly teach displaying actions taken by the operator for the particular event. However, this is taught by Central Point, on pages 46-47.

At the time of the invention, it would have been obvious to combine the teachings of Central Point with the Billhartz combination. One of ordinary skill in the art would have been motivated to perform such an addition to create such records for data logging and for future references. This is taught on page 46 of Central Point, where it teaches that logs may be used for future references.

10. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper, Symantec, and Billhartz, as applied above, and further in view of Kuroshita US Patent No. 5,550,807 (hereinafter Kuroshita).

As per claim 20, displaying network statistics is taught throughout Cooper, such as in Figure 20. Although the Cooper combination teaches displaying many different statistics, the references do not explicitly teach displaying a ranking of hosts in the network according to a network statistical measure. Ranking hosts according to network statistical measures are taught by Kuroshita though, such as in col. 1 line 34-52.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to combine the teachings of Kuroshita with the Cooper combination. One of ordinary skill in the art would have been motivated to perform such an addition to manage the network and standardizing a network management protocol. This is taught by Kuroshita in col. 1 lines 52-53.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jason K. Gee whose telephone number is (571) 272-6431. The examiner can normally be reached on M-F, 7:00 am to 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-38383811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jason Gee
Patent Examiner
Technology Center 2100
02/07/2008

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER